Public Safety Wireless Network

PSWN

Security Field Data Collection & Analysis Report

Site #1 800 MHz Analog Trunked Radio System

Final

October 1998

FOREWORD

This report presented by the Public Safety Wireless Network (PSWN) program documents security issues and candidate recommendations identified during the first of a series of security field data collection and analysis efforts. The primary goals of these efforts and the resulting reports are to raise security awareness and understanding and to help mitigate security risks associated with evolving public safety communications systems.

Questions or comments regarding the information contained in this document should be forwarded to the PSWN Program Management Office (PMO) at 800-565-PSWN. For more information regarding the purpose and goals of the PSWN program, see the PSWN web site at www.pswn.gov.

TABLE OF CONTENTS

Page

1. INTRODUCTION

The Public Safety Wireless Network (PSWN) program has deployed case study teams to conduct detailed interviews with managers and users of public safety radio systems in selected regions of the United States. The case study interview guides used by these teams include several security-related questions. The PSWN program also has initiated a number of security-focused data collection and analysis activities. These data collection activities build on the security information gathered through the case studies by collecting more detailed security information at a few selected sites. A *Security Field Data Collection Summary Report* will be prepared at the conclusion of the initial series of security-focused data collection efforts. These efforts support the larger goal of establishing the PSWN program as a valuable information resource and a source of guidance for many aspects of public safety communications.

On October 8, 1997, an Emergency Communications Center (ECC) serving police, fire, and emergency medical services became the first site visited under the security data collection and analysis effort. This report documents the results of that effort. All references to the agency visited have been removed from the report.

When conducting a site visit, the PSWN team uses an internally prepared security data collection plan as a guide to ensure all pertinent information is collected. Site visits provide the PSWN team an opportunity to improve the plan based on lessons learned following each visit. This process ensures the PSWN team requests the latest, most accurate, security relevant information at subsequent site visits.

1.1 Purpose

The security field data collection activities will increase understanding of the emerging security issues associated with evolving public safety communications infrastructures. These efforts also will provide insight into the risks associated with the computerization and digitization of those infrastructures as well as the security concerns and needs of the public safety community. In addition, the studies will identify best security practices and measures taken to decrease the risk to public safety radio components and information.

Security field data collection activities support the following goals:

- Identifying the sensitivity levels of data communicated
- Documenting communications infrastructures used, including wireless and wireline connectivities
- Describing existing technical and procedural security controls

- Identifying security concerns, as well as the frequency and nature of known security issues and incidents
- Capturing existing best security practices and security measures.

Additional security issues, concerns, and practices will be documented as data are collected at additional public safety agency sites. Those findings, as well as the findings in this report, may reveal patterns or commonalities in the security of public safety communications. Dissemination of security issues, best practices, and candidate recommendations to the public safety community should provide valuable guidance as the community makes decisions about the security of its systems.

1.2 Scope

The security-focused field data collection is intended to gather security-related data on public safety communications infrastructures to enhance the understanding of possible risks to these infrastructures. This report is not an evaluation of the security practices of any particular public safety agency or of public safety communications infrastructures in general. Candidate recommendations are included for each security issue identified in the report. These recommendations and new candidate recommendations will continue to be evaluated during subsequent data collection activities for potential inclusion in a summary report.

1.3 Document Organization

This document is divided into the following sections:

- Section 1, Introduction—Presents background, purpose, scope, and document layout.
- Section 2, Approach—Describes the approach used in conducting the security field data collection and analysis.
- Section 3, System Description—Presents a description of the system analyzed and the organization visited.
- Section 4, System Security Findings—Presents issues identified during the data collection effort and any best practices used by the subject organization to secure its system.
- Section 5, Summary—Provides a synopsis of the findings discussed in the previous section and highlights potential security misperceptions.
- Appendix A, Acronyms—Contains a list of acronyms used in this report.

2. APPROACH

This section describes the approach used in conducting this security field data collection and analysis effort. Subsequent data collection efforts will follow a similar approach and will be conducted in accordance with a data collection plan containing several security questionnaires. The use of the data collection plan will ensure consistency across site interviews and adequate coverage of security.

Step 1: Coordinate and prepare for data collection effort

- Identify personnel for conducting the security data collection effort
- Coordinate the data collection schedule
- Determine which site personnel should be interviewed
- Identify the type of system components at the site for pre-interview research
- Prepare a list of questions for use during the interviews.

Step 2: Collect system and site data

- Validate system information collected in Step 1
- Collect more detailed information about the site's system configuration including a system diagram if possible
- Identify current security practices, concerns, and needs.

Step 3: Research and clarify data gathered from the site

- Collect data from various sources (e.g., Internet, professional journals) concerning security issues and concerns raised
- Recontact the site, if necessary, to clarify information gathered.

Step 4: Analyze and document security issues, candidate recommendations, and best practices

- Describe the security issues raised during data collection
- Provide candidate countermeasure recommendations, as applicable, for security issues
- Document existing best practices at the site
- Consolidate the site data and their analysis into a report.

3. SYSTEM DESCRIPTION

The ECC serves as the 9-1-1 emergency reporting center for a county and as the dispatch center for police, fire, and emergency medical service (EMS) units. The center is staffed by approximately 50 trained professional personnel.

The ECC's main communications are supported by a mobile radio system with a third-generation Computer-Aided Dispatch (CAD) system. The ECC system includes a 15-channel 800 Megahertz (MHz) trunked analog radio system using four simulcast transmitter sites. Three of the 15 channels are equipped to support secure communications through a Digital Voice Privacy (DVP) feature. Figure 1 provides an overview of the 800 MHz system and a high-level view of mobile data terminal (MDT) connectivity. The ECC also simulcasts its police and fire department primary channel communications on ultra high frequency (UHF) conventional analog systems. A dedicated system using another UHF frequency is used for MDT traffic. Augmenting the primary center is a backup auxiliary operations center (AOC) maintained at a fire station. In addition, the police department's mobile command post vehicle contains a fully functional communications area with the following equipment:

- Very high frequency (VHF), UHF, and 800 MHz radios
- Computer-aided dispatch terminal
- Scanner monitor radio
- Cellular telephones
- Hardwired telephones and 9-1-1 telephones
- MDT
- Facsimile (FAX) machine and copier.

The system's primary radio frequency (RF) site has primary and backup prime site controllers. The backup prime site controller immediately gains control of the system if the primary controller goes down. The AOC, shown as Remote RF Site #2 in Figure 1, contains a prime site controller in cold standby mode. The AOC is activated if the primary RF site goes down. The cold standby-system's subscriber database is kept current with the primary RF site database to ensure that operations are minimally affected when the AOC assumes control. Uninterruptible power supplies and generator backup power are provided at all RF locations and at the ECC. Each site also contains entry, heat, and smoke alarms that send a notification to the ECC under the appropriate conditions. Access to the ECC is controlled by requiring entrance through two cipher lock enabled doors, remote sites are all physically secured by a combination of locked doors and controlled access to the spaces they occupy (e.g., on the upper floor of an office building).

The ECC is connected to the rest of the 800 MHz communications system by digital microwave radio. Control and management of the 800 MHz radio system are performed by the ECC radio system manager. The radio system manager uses a network management system and system- monitoring software to configure, control, and monitor the system. Both of these systems are hardwired to the primary RF site. In addition, there is dial-in access to a computer to allow the radio system manager to control the radio system remotely when required. Dispatchers can perform dispatch-related control of the radio system from the dispatch console. The simulcast and MDT communications systems are connected to the ECC via conventional analog UHF elements co-located with the 800 MHz system components.

4. SYSTEM SECURITY FINDINGS

This section describes the security issues and the best practices identified during the site visit and in subsequent research. It includes a table that maps each security issue to one or more data collection sources.

4.1 Security Issues

The security issues described in this section include possible implications or associated risks along with candidate recommendations on mitigating the risks. Table 1 summarizes the identified security issues and the corresponding recommendations. The following subsections provide more details. Table 2 lists the data sources used in identifying the security issues and the best practices.

Table 1
Summary of Security Issues and Candidate Recommendations

Section	Security Issue	Candidate Recommendation
4.1.1	Scanners are a concern.	Agencies should be made aware that all conventional or trunked analog unencrypted communications are vulnerable to interception and monitoring using low cost, commercially available radio scanners.
4.1.2	Primary channels transmitted in the clear.	Agencies with trunked systems that transmit information on a clear conventional analog channel for the benefit of the public or press should establish operating policies that move communications from the clear channel to an encrypted channel (if available) or tactical talk group as soon as possible. Agencies should remain vigilant in identifying incidents in which interception and misuse of unprotected information has jeopardized any operation.
4.1.3	MDT transmission interception is a concern.	Agencies using MDTs to communicate sensitive information over unencrypted channels should consider employing encryption techniques.
4.1.4	Encryption-capable radios are not used in encrypted mode.	Agencies should ensure that security mechanisms will not significantly interfere with operations. They should ensure that mechanisms are configured properly and that users receive sufficient training.
4.1.5	System dial-in capability could be exploited.	Network managers should be made aware of network dial-in vulnerabilities and secure practices (e.g., modem dial-back, token-based authentication, password parameter settings). Security policies should address this remote management and maintenance point of entry.
4.1.6	Data integrity is a greater concern than data confidentiality.	Data integrity and confidentiality concerns should be considered as the development of comprehensive security requirements and guidelines progresses.

Table 2
Data Collection Sources

Data Collection Source	4.1.1	4.1.2	4.1.3	4.1.4	4.1.5	4.1.6	4.2.1
Site interview	•	•	•	•	•	•	•
ECC web site							•
Internet newsgroups	•						
Scannerists' Internet web sites		•					
Scannerists' publications	•						
Public safety publications			•				
Site/radio system vendor correspondence			•				
Vendor system documentation							•

4.1.1 Scanners Are a Concern

The use of radio scanners by hobbyists, the public, and the press to listen to public safety communications has existed for some time. In the past, this recognized activity has been of little concern to the public safety community since no harm has resulted to public safety officials. Seizures of computers and radio scanners used by criminal elements to monitor police communications is changing the perception that monitoring public safety communications is a benign activity. Additionally, more detailed information concerning private citizens is being sent over unprotected public safety wireless systems and networks thus supporting the need for some form of protected wireless system. In instances where public safety agencies have installed fully encrypted radio systems or used other technologies (such as trunking) that have prevented the use of radio scanners, the press has challenged the use of these technologies by arguing the public has a right to know.

With the introduction of trunked radio systems, many public safety officials were lulled in a false sense of security with the knowledge that earlier radio scanners could not follow the communications associated with trunked systems. However, multiple vendors have since developed scanners capable of tracking trunked analog communications. Review of various Internet newsgroups has revealed that these products are in use.

In addition, public safety frequencies are readily available on the Internet and through other sources. A scanner newsgroup entry noted that a "National Public Safety Trunked System Frequency Guide" is included with the purchase of a trunking scanner. In addition, a particular newsgroup has published the public safety frequencies for the county in which the ECC is located along with instructions for programming the trunking scanner to monitor specific talkgroups. In another newsgroup, when an individual requested a list of a certain county's Police Department frequencies, the response included the type of land mobile radio (LMR) system used by that department, the type of scanner needed (trunking), and an offer to provide the names of user groups.

Although trunking has not been considered a security feature, it has been perceived as providing an additional level of obscurity for "hiding" communications traffic. Agency personnel had considered their voice communications to be unavailable to the general public because of trunking. Until the development of the trunk-tracking scanners, this perception was correct; average citizens did not have the ability to follow complete, coherent conversations. However, the advent of trunk-tracking scanners has enabled the average citizen to follow such conversations, making the communications available to anyone with the new scanner and knowledge of the appropriate frequencies. A related misconception identified during this data collection is that users perceive the "private call" radio feature, in which two radio users may talk on their own frequency, as being secure. These conversations can be scanned just as readily as any other clear communications.

Candidate Recommendation:

Public safety agencies should be made aware that all unencrypted analog communications, voice or data, conventional or trunked, are susceptible to interception and monitoring at any point in a land mobile radio system. Radio users should also be made aware that the "private call" feature does not offer voice privacy or security. Agencies installing digital land mobile radio systems should remain vigilant when permitting unencrypted digital communications on the system. The use of end-to-end encryption can lessen the probability of public safety communications being intercepted by unauthorized personnel.

4.1.2 Primary Channels Transmitted in the Clear

The ECC transmits its police and fire department primary channel communications in the clear on a UHF conventional analog system as well as on their trunked 800 MHz analog system. Depending upon the sensitivity and extent of the information being communicated on this channel and the intent of the listener, some degree of security risk may exist for public safety operations and privacy information may be disclosed to unauthorized individuals. For example, the concern was recently raised about the interception and misuse of apartment entry codes transmitted in the clear. To mitigate this potential security issue, public safety personnel have been told to use their MDTs to communicate sensitive information as a secure alternative, although, as described in Section 4.1.3, MDT traffic may also be a vulnerable avenue of communications.

Candidate Recommendation:

Public safety radio users should move from the primary channel to a tactical channel as soon as possible to reduce the chance of exposing sensitive communications. However, to ensure the confidentiality of tactical channel communications, encryption should be employed. Agencies should remain vigilant in identifying incidents in which the interception and misuse of any clear information has jeopardized critical missions or endangered citizens.

4.1.3 MDT Transmission Interception is a Concern

An individual anonymously posted information on the Internet claiming the ability to convert a proprietary mobile data protocol in order to intercept and interpret mobile data transmissions. They also indicated the possibility of spoofing (i.e., transmit with the appearance of being sent by an authorized user of the system) message data on an MDT network. An MDT.exe C++ software program was posted. An issue of a trade publication documented this Internet posting.

An ECC administrator raised the issue within his agency and with the vendor to determine whether the information was accurate, what concerns the agency should have, what actions could or should be taken, and whether the vendor could provide additional information. The vendor's response basically stated that voice and data wireless transmissions are not immune to hacker attacks. The vendor noted that wireline computer users have confronted the same problem for years. They did, however, downplay the risk of unauthorized MDT interception, noting that the technical sophistication required to send data on a mobile data system would make it unlikely.

An article in a subsequent issue of the trade publication stated that the MDT hacker software works but the packets are unsorted. According to the article, transmission packets are received out of order, so reconstruction of a message may be difficult on a busy system.

The data that are transferred between an MDT and local and national databases are typically unencrypted. For the ECC, data are transmitted on a dedicated, UHF frequency and include the following types of information:

- Driver's license information
- Motor vehicle information
- Local records
- Local criminal information network data
- National Crime Information Center (NCIC) data.

On the basis of the information discussed, it is believed that the current security risk associated with the interception of MDT traffic is likely to be low. However, unencrypted MDT traffic is no more secure than unencrypted voice traffic. As has occurred with the development of trunking scanners, it appears that devices and software will become available to the general public to enable MDT traffic to be easily monitored.

Candidate Recommendation:

Agencies using MDTs to communicate sensitive information over unencrypted channels may want to consider employing encryption techniques. It is only a matter of time before methods for monitoring unencrypted MDT traffic are publicly available. In addition, when procuring wireless data services through commercial providers offering "encryption", agencies

should closely examine the type and level of encryption being offered to determine if it is sufficiently secure for their needs. If the algorithm used is not DVP or DES, the encryption scheme may be trivial to break by determined individuals.

4.1.4 Encryption-Capable Radios Are Not Used in Encrypted Mode

The agency's vice squad requested and received radios with encryption capability. In addition, system resources were dedicated to support this capability. After some time, the radio system manager observed that the dedicated system resources allocated for use by the vice squad were not being used. When queried, vice squad personnel indicated that the voice quality was degraded when using the radios in the encrypted mode. It was their perception the encrypted radios just "didn't work" as well as those without this capability. Although the vice squad recognized the need to protect their communications, they chose to operate in the clear rather than jeopardize their operations when operating in the encrypted mode.

Many users of analog radio systems complain of poor voice quality when operating in the encrypted mode. Users have also complained of a reduction in range when using encryption. These are known technical issues effecting analog radio systems when encryption is introduced. The impact of these problems can be lessened but not totally eliminated. User confidence can be enhanced through proper training. Although the transition from analog to digital communications may itself introduce some degradation in range and voice quality, the introduction of encryption into digital radio systems should not affect range or voice quality.

Candidate Recommendation:

Agencies should ensure that any new security mechanism will allow their personnel to do their jobs in the same way that they do them with current equipment. In addition, an agency should ensure that it receives proper instruction from the vendor and assurance of the proper configuration of mechanisms (based on the agency's security policy, if one exists). Users, in turn, should be trained in the proper use of the security mechanisms.

4.1.5 System Dial-in Capability Could Be Exploited

The ECC's dispatch network has a dial-in capability that radio system administrators use for remote administration. The ECC dispatch network includes connectivity to the local area network within the ECC building, a larger wide area network, and remote databases. These interconnections introduce the possibility that intruders who gain access to a host on the network could greatly expand their access by exploiting vulnerabilities.

The telephone number for the dial-in entry point is an unpublished number known only to a few ECC personnel. However, commonly used automated tools called wardialers could exploit this point of entry. Wardialers are used to identify modems among a range of phone numbers. They may be configured to repeatedly attempt to login to a remote computer, once a modem connection is made, using numerous user IDs and a dictionary of possible passwords.

The identification and authentication controls used for this entry point consist of various screen names and passwords. Each screen name has a separate password associated with it. The screen names are the same names that are associated with the screens when they are used on-site. Therefore, limiting the distribution of the password for a particular screen can enforce restriction to certain functions (e.g., menu choices on the screen). The passwords are not strong. They consist of no more than eight letters, and no numbers or special characters are used. In addition, the passwords have not been set to expire and have not been changed since the system was installed 6 years ago. After three unsuccessful login attempts, further attempts are prohibited until 30 seconds has elapsed, a report is generated, and the report is sent to the printer. Such a report could go unnoticed for a day or more because the printer is not frequently checked.

Most significantly, this entry point provides an avenue through which many aspects of the radio system can be modified or deleted. A talkgroup could have its name or membership and its mappings of frequencies to talkgroups modified, and the whole system could be shut down or made unusable by a determined hacker.

Candidate Recommendation:

Awareness of the potential vulnerabilities associated with various network access methods should be raised in the public safety community because it is likely that similar remote access "conveniences" exist on other public safety communications networks. Security safeguard options should be considered by network managers to mitigate the risk of such vulnerabilities (e.g., modem dial-back, token-based authentication, password configuration constraints).

4.1.6 Data Integrity Is a Greater Concern Than Data Confidentiality

ECC administrators rated data integrity as a higher priority than confidentiality. In other words, the communication of accurate information (i.e., sender identity and the message transmitted are understandable and unchanged from the origination point) is vital to the site's mission-critical operations. Protecting "privacy information" in databases from unauthorized disclosure and protecting that information en route, although important, are considered secondary concerns.

As described in Section 4.1.3, it is possible to intercept MDT transmissions. It is implied in the resource information analyzed that it is also possible to masquerade as an authorized user of an MDT and to construct phony messages. Because there has been no proven ability to adequately intercept messages, and the insertion of phony messages is much more complex and difficult than is implied in the resource material, it appears that the risk of phony messages being inserted into a system is insignificant at this time. However, as an added precaution, the ECC has notified MDT users to be wary of unusual message traffic (for instance, when messages that appear to have originated from specific MDTs but the MDT operators indicate that they did not send the messages).

Candidate Recommendation:

The capability of masquerading as an authorized MDT user should continue to be monitored. Additional methods of providing data integrity for MDT transmissions should be investigated.

4.2 Best Security Practices

The "best security practices" presented in this section include concepts, designs, and procedures that appear to be reasonable methods of mitigating security risks to public safety communications infrastructures. Each best practice includes a description of the practice and the threat(s) that it counters.

4.2.1 System Reliability and Availability Should be Ensured

System availability and reliability can be increased through the use of infrastructure redundancy, the technical ability to continue communications in a degraded state, and contingency plans and procedures.

Infrastructure redundancy and the ability to continue communications in a degraded state are often linked together and provided by many vendors' radio systems For example, the ECC's hot standby prime controller provides redundancy of equipment that enables the system to operate normally even if the prime controller fails. Its backup cold standby controller at the AOC provides for degraded operations by performing limited trunking operations (with the other two sites reverting to local failsoft operations) in case both the main and hot prime controllers fail. The multiple consoles in the ECC also act as redundant equipment with the dispatching console at the AOC acting as a degraded state option if equipment failures are encountered.

The preparation and use of contingency plans and procedures ensures that public safety personnel remain proficient in providing service under adverse conditions. The ECC's contingency plan covers both localized equipment failures and environmental conditions requiring relocation of emergency communications. As described in the previous paragraph most local equipment failures are handled by the vendors' equipment and design. For evironmental conditions, the ECC, exercises its AOC on a monthly basis to ensure its viability and ECC personnel's familiarity with their roles and responsibilities.

5. SUMMARY

This section provides a synopsis of the security issues presented in Section 4, highlighting potential security misperceptions.

The security issues identified during the first site visit and through subsequent information gathering are summarized as follows:

- Unencrypted communications are vulnerable to interception and monitoring using low cost, commercially available radio scanners. Neither trunking nor the use of the "private call" feature provide any reliable degree of security.
- MDT transmission conversion is possible and would allow a hacker to determine the contents of MDT traffic.
- Encryption capable radios are not used in the encrypted mode, negating the value of the encryption.
- The dial-in capability of the system and the lack of added security measures for controlling that connection, leave the system open to potential exploitation.
- Data integrity (i.e., ensuring that the data and the identity of the sender of a transmission have been unaltered) is more important than ensuring the privacy of the data.

Two of the security issues identify areas in which potential misperceptions of security may exist. The first issue concerns a possible perception that trunking provides a level of security for communications. As stated in Section 4.1.1, trunk-tracking scanners are readily available. The second issue involves the perception that mobile data transmissions are secure. Although current indications are that discerning the content of MDT messages is not easy, the ability does exist to convert the content of such messages and eventually a method will be developed to make that content understandable. Therefore, MDT transmissions should not be considered secure. Security misperceptions will continue to be tracked and documented in subsequent reports.

APPENDIX A

Acronyms

AOC	Auxiliary Operations Center
CAD	Computer Aided Dispatch
DVP	Digital Voice Privacy
ECC	Emergency Communications Center
EMS	Emergency Medical Service
FAX	Facsimile
LMR	Land Mobile Radio
MDT	Mobile Data Terminal
MHz	Megahertz
PMO	Program Management Office
PSWN	Public Safety Wireless Network
RF	Radio Frequency
UHF	Ultra High Frequency
VHF	Very High Frequency